A

REDACTED

B

REDACTED

C

REDACTED

D

REDACTED

E

REDACTED

F

REDACTED

G

REDACTED

H

REDACTED

I

REDACTED

J

REDACTED

K

SITEPROTECTOR™

SecurityFusion Module Guide

Version 2.0, March 8, 2006

Overview

Introduction

This guide provides information about installing and configuring SecurityFusion Module 2.0 to work with SiteProtector 2.0, Service Pack 6.0.

Audience

This guide is primarily for IT/security administrators, security managers, and implementation analysts who are responsible for the installation and configuration of the SecurityFusion Module with Site Protector.

In this document

This document contains the following sections:

EXHIBIT
334
gwp 4.19.06

SECTION A: Introduction to the SecurityFusion Module

Overview

Introduction This section provides an introduction to the SecurityFusion Module.

In this section This section contains the following topics:

What is the SecurityFusion Module?

Introduction

This topic describes the SecurityFusion Module.

Description

The *SecurityFusion Module* is a separately purchased product for SiteProtector that provides additional security functionality. The module increases your ability to quickly identify and respond to critical threats at your Site. Using advanced correlation and analysis techniques, the Module escalates high impact attacks and critical attack patterns to help you focus on the most important attack activity.

How it works

When an intrusion detection agent detects an attack, the SecurityFusion Module does the following:

- increases your ability to quickly identify and respond to critical threats at your Site
- escalates high impact attacks and critical attack patterns to help you focus on the most important attack activity
- correlates events from intrusion detection/prevention agents with events from scanning agents
- correlates the attack with information about the host, such as operating system, vulnerabilities, and responses taken by host agents, to determine the success or failure of the attack
- recognizes patterns of event activity that indicate serious security incidents, such as targeted and network break-in attempts or attack activity from compromised hosts
- consolidates the patterns into single incidents, which makes dealing with streaming event data much more manageable

Components

Table 1 describes the components of the SecurityFusion Module:

Component	Description
Impact analysis	Impact analysis correlates intrusion detection events with vulnerability assessment, operating system, and sensor-blocking messages, so that it can immediately estimate the impact of the an individual event.
Attack pattern	Attack patterns recognizes patterns of events that indicate attacks, such as unauthorized scans, break-in attempts, and activity from compromised hosts.

Table 1: *SecurityFusion Module component descriptions*

The SecurityFusion Setup Process

Introduction

This topic provides an overview of the stages of the SecurityFusion Module process.

Requirement

Before you install and configure the SecurityFusion Module, you must complete the tasks for setting up SiteProtector and the agents that work with SiteProtector. For information about this process, see the *User Guide for Security Managers*.

Process

Table 2 describes the stages of the SecurityFusion Module setup process:

Stage	Description
1	Installation: Install the SecurityFusion Module on a dedicated computer that does not include any other SiteProtector software. See "Installing the SecurityFusion Module" on page 7.
2	Configuration: • Configure a custom policy for the SecurityFusion Module that includes the assets monitored by the Module. See "Configuring Policies" on page 13. • Configure a custom response for the SecurityFusion Module. See "Configuring Responses" on page 21. • Configure additional parameters for the SecurityFusion Module. See "Additional Configuration Tasks" on page 29.

Table 2: *Stages of the SecurityFusion Module setup process*

SECTION B: Installing the SecurityFusion Module

Overview

Introduction

This section explains how to install the SecurityFusion Module.

In this chapter

This chapter contains the following topics:

Evaluating the Module

You can install the SecurityFusion Module for evaluation purposes and operate without purchasing a license agreement, as follows:

- The evaluation period is 90 days.
- The full functionality of the Module is available.
- The Module generates periodic messages indicating the number of days left in the evaluation period.
- At the end of the evaluation period, you must purchase a license agreement to continue using the Module.

Before You Begin

Introduction

This topic defines the information you must obtain and the tasks you must perform before you install the SecurityFusion Module.

Prerequisites

Before you install SecurityFusion Module, you must complete the following tasks:

- Install and configure SiteProtector.

  See the *SiteProtector Installation Guide* and *SiteProtector User Guide*.
- Verify that you have administrative rights to the SiteProtector Database and Application Server.
- Choose a computer for the SecurityFusion Module. You must install the Module on a separate, dedicated computer that does *not* include other SiteProtector software.
- Verify that the computer where you are installing the SecurityFusion Module meets the system requirements.

  See the *SiteProtector System Requirements*.
- Obtain a license for the SecurityFusion Module. If you do not have a license for the Module, then you can run the program in evaluation mode until you obtain a license.
- Determine whether to use Windows or SQL Authentication to the SiteProtector Database.

  Note: If you choose Windows Authentication, you must install the SecurityFusion Module with the separate installation package; if you choose SQL Authentication, you may install from the Deployment Manager or the installation package.

Installation methods

Table 3 describes the methods for installing the SecurityFusion Module:

Method	Description
Deployment Manager	To install the product from the Internet, start Internet Explorer, and then go to the Deployment Manager. **Example:** `https://ip_address_or_server_name:3994/deploymentmanager/`
Separate Installation Package	You can obtain the installation package from the following locations: • the ISS Web site `http://www.iss.net/download/` • the SecurityFusion folder on the ISS product CD.

Table 3: *Methods for installing SecurityFusion Module*

SecurityFusion Licenses

Introduction

Your license agreement for the SecurityFusion Module allows you to protect a specific number of hosts with SecurityFusion correlation. A license enables both impact analysis and attack pattern correlation. You must specify which assets can use SecurityFusion licenses in the SecurityFusion policy.

Important: The Module will not correlate events until you specify hosts.

How the Module allocates licenses

The Module allocates licenses at startup based on the following:

- the order in which hosts are specified for licensing in the SecurityFusion policy
- SiteProtector knows of the host because of one of the following:
  - The host belongs to a group in Site Manager.
  - A scan performed by the Network Internet Scanner and Network Enterprise Scanner identified the host.
  - SiteProtector received an event for which the host was either the source or the target.

License compliance

To understand more about SecurityFusion licenses, see the Help in the SecurityFusion policy.

Guidelines for proxy servers

If you use a proxy server for internet access, you should not include the IP address of the server in your list of hosts. If you do, you may see the following false alarms:

- Traffic into the proxy may be interpreted as incoming attacks directed at the proxy.
- Traffic out of the proxy may be interpreted as outgoing attacks originating at the proxy.

Including a proxy for SecurityFusion correlation can cause false alarms in either of the following cases:

- The proxy is both the source and the target of the attack.
- The source of the attack is a licensed IP address, and the target of the attack is the proxy.

Using DHCP addresses

When you use DHCP, IP addresses are assigned randomly and a host may use different IP addresses for each network log on. Random assignment of IP addresses may affect your use of licenses. The exact impact at your Site depends on the size of the range and the number of hosts that use the range.

ISS recommends that you use static IP addresses for critical hosts and purchase enough licenses to cover all IP addresses in the range used by DHCP.

Installing from the Deployment Manager

Introduction

This topic explains how to install the SecurityFusion Module with Deployment Manager.

Procedure

To install the SecurityFusion Module with Deployment Manager:

1. On the computer where you want to install the Module, start Internet Explorer, and then go to the Deployment Manager.

   Example:

   `https://ip_address_or_server_name:3994/deploymentmanager/`

   The Deployment Manager Main Menu appears.
2. Click **Install the SiteProtector Security Fusion Module.**

   The Prerequisites page appears.
3. Verify that the computer meets the prerequisites, and then click **Next.**

   The SQL Server Information page appears.
4. Provide connection information for the SQL Server instance running the SiteProtector database, and then click **Next.**

   The Prepare to Install page appears.
5. Review the information on the Prepare to Install page, and then click **Install.**

   The File Download window appears.
6. Select the **Run this program from its current location** option, and then click **OK.**

   The Security Fusion Module installation begins.
7. You must complete at least the minimum configuration tasks to make the Module function.

   Reference: See the *SiteProtector User Guide for Security Managers*, Chapter 10, "Configuring the SecurityFusion Module."

Installing the Module from Separate Installation Packages

Introduction

This topic explains how to install the SecurityFusion Module from a separate installation package.

Obtaining the package

You can obtain a separate installation package for the SecurityFusion Module from the following locations:

- the ISS Web site `http://www.iss.net/download/`
- the ISS product CD in the `\SecurityFusion` folder.

Procedure

To install the SecurityFusion Module from a separate installation package:

1. On the computer where you want to install the product, start the installation program.

   The InstallShield Wizard appears.
2. Follow the onscreen instructions to complete the installation process.
3. You must complete at least the minimum configuration tasks to make the Module function.

   Reference: See the *SiteProtector User Guide for Security Managers*, Chapter 10, "Configuring the SecurityFusion Module."

SECTION C: Configuring Policies

Overview

Introduction

This section provides information about configuring SecurityFusion Module policies, including how to define assets in the policy.

Requirement

You must configure and apply a custom policy for SecurityFusion Module before the Module will function properly. The policy must include the following information:

- the assets protected by the SecurityFusion Module

  See "Defining Assets in SecurityFusion Module Policies" on page 16.
- response policies

  See "Configuring Responses" on page 21.
- parameters for attack patterns

  See "Additional Configuration Tasks" on page 29.

Task overview

Table 4 describes the tasks for configuring the SecurityFusion Module policies:

Task	Description
1	Configure the custom SecurityFusion Module policy. See "Configuring and Applying Custom Policies" on page 15.
2	Define assets in the custom policy. See "Defining Assets in SecurityFusion Module Policies" on page 16.
3	Apply the custom policy. See "Configuring and Applying Custom Policies" on page 15.
4	Verify that the SecurityFusion Module is working.

Table 4: *Tasks for configuring SecurityFusion Module policies*

Related documentation

For information about creating and applying SecurityFusion Module policies and responses, see the following:

- *SiteProtector User Guide for Security Managers*
- *SiteProtector Help*

In this section

This section contains the following topics:

Configuring and Applying Custom Policies

Introduction

This topic provides instructions for configuring custom policies based on the existing, predefined policies included with SiteProtector.

Important: You cannot change the original, predefined policy.

Environments

SiteProtector provides predefined policies for the Windows environment.

Before you begin

Before you configure and apply custom policies for the Module, make sure the Module appears in the SiteProtector Console with a status of *Active*.

Configuring custom policies

To configure a custom policy for the SecurityFusion Module:

1. In the left pane, right-click the Site Node that contains the SecurityFusion Module, and then select **Manage Policy** from the pop-up menu.

   The Policy tab appears.
2. Right-click the SecurityFusion Module policy, and then select **Derive New** from the pop-up menu.

   The Derive New Item window appears.
3. Type the name for the custom policy, and then click **OK**.

   The Common Policy Editor appears.
4. Edit the policy in the Common Policy Editor.

   For more information about using the Common Policy Editor, refer to the Common Policy Editor Help.
5. Save the policy.

   The policy is available for you to apply to the SecurityFusion Module.

Applying policies

To apply a policy to SecurityFusion Module:

1. In the left pane, select the group that contains the SecurityFusion Module.
2. In the **View** list, select **Agent**.
3. In the right pane, right-click the agent, and then select **Apply→ Policy** from the pop-up menu.

   The Apply Policy window appears. The Command Details section lists the Action (Apply Policy), the Asset where the agent is installed, and the Agent Type.
4. Click the **Policy** icon, and then select a policy from the list.
5. Click the **Schedule** icon, and then select **Run Once** to apply the policy immediately or schedule a job to apply the policy.
6. Click **OK**.

Defining Assets in SecurityFusion Module Policies

Introduction

This topic provides information about defining assets in the SecurityFusion Module policy, including the following tasks:

- defining assets with single addresses
- defining assets with multiple IP addresses
- importing assets from host files
- deleting assets from the policy to make licenses available to other assets or to remove assets that are no longer on the network

Methods

Table 5 describes the methods for defining assets in the SecurityFusion Module policy:

Method	Description
Manual	Use this method to type asset information in the policy manually. You must follow strict format requirements for IP address and host names. You can use this method to define assets with multiple IP addresses in the policy.
Automatic	Use this method to import asset information into the policy automatically from a host file (`.hst`). The information in the host file must meet format requirements.

Table 5: *Methods for defining assets in the SecurityFusion Module policy*

IP address requirements

IP addresses must meet the following requirements:

- Each IP address must be valid, otherwise the Module generates an error message. For example, if the user enters a DNS name for a computer that cannot be resolved to an IP address, the user will get an error message.

  Note: Each IP address does not have to be in use. As long as there is a record in the DNS internal or external network, the Module will be able to resolve the IP address correctly.

Allowed formats and examples

Table 6 describes the allowed formats for IP addresses and provides examples:

Type	Allowed Formats	Examples
single IP address	IP address in dotted decimal notation	1.1.1.1
	IP address that includes a wild card (*)	1.1.1.*
	IP address in CIDR format	1.1.1.1/24
	DNS name	host-a.example.microsoft.com
	computer name[a]	MailServer01
	Web address[b]	www.iss.net
range of IP addresses	the first and last IP address separated by a hyphen	1.1.1.1-1.1.1.100 1.1.2.1-1.1.3.1

Table 6: *Allowed formats for IP addresses and examples*

a.The Module translates the computer name into an IP address.

b.The Module translates the Web address into an IP address.

Defining assets manually

To define an asset in the SecurityFusion Module policy manually:

1. Open the custom SecurityFusion policy for editing.
2. In the left pane, select **Host Configuration**.
3. In the right pane, type the names and addresses of your assets in the **Enter IP addresses and/or Host names to validate** box.

   Important: The format of the addresses must meet the requirements as defined in this topic.
4. Click **Validate IPs**.

   The valid IP addresses move to the **The following hosts are available for SecurityFusion correlation** box.
5. If there were any errors in your IP addresses, correct those errors, and then repeat Step 4.

Assets with multiple IP addresses

The SecurityFusion Impact Analysis Component can correlate events that occur on multi-homed systems, or systems that have more than one network interface card. By default, SecurityFusion treats each IP address as a separate host, but you can configure SecurityFusion to treat multiple IP addresses as a single host to correlate events that occur on those IP addresses.

Defining assets with multiple IP addresses

To define an asset with multiple IP addresses:

1. Open your custom SecurityFusion policy for editing.
2. In the left pane, select **Host Configuration**.
3. In the right pane, scroll to the **Multi-Homed Systems (MHS) Configuration** box.
4. Click **Add**.
5. On the **MHS Configuration** dialog, type a host **Name**.
6. Type two or more **IP Addresses**, separated by commas or hard returns, and then click **OK**.
7. Repeat Steps 4 through 6 to add more multi-homed systems.
8. On the **File** menu, select **Save**, and then click the **Close** button.

   Note: If you did not modify the active policy, you must manually apply the policy to make it active.

Host files

If you already have a Host File (`.hst`) available, then you can import lists of assets from the file into SecurityFusion. You can generate a host file with Internet Scanner or create one yourself. For either method, use the formats for host names and addresses as explained earlier.

Importing assets from host files

To import assets from a host file:

1. Open your custom SecurityFusion policy for editing.
2. In the left pane, select **Host Configuration.**
3. In the right pane, click **Import Host File.**
4. Locate the host file (`.hst`), and then click **Import.**

   The content of the file appears in the **Enter IP addresses and/or Host names to validate** box.
5. Click **Validate Hosts.**

   The valid IP addresses move to the **The following hosts are available for SecurityFusion correlation** box.
6. If there were any errors in your IP addresses, correct those errors, and then go to Step 5.
7. On the **File** menu, select **Save**, and then click the **Close** button.

   Note: If you did not modify the active policy, you must manually apply the policy to make it active.
8. On the **File** menu, select **Save**, and then click the **Close** button.

   Note: If you did not modify the active policy, then you must manually apply the policy to make it active.

Deleting assets from the policy

To delete assets from the SecurityFusion Module policy:

1. Open your custom SecurityFusion policy for editing.
2. In the left pane, select **Host Configuration.**
3. In the right pane, select the host(s) that you want to delete in the **The following Hosts are available for SecurityFusion correlation** box, and then click **Delete.**

   The host(s) is deleted.

   Note: You can only delete a line of hosts. If the line contains hosts that you do not want to delete, you must delete the line, and then add back the hosts to keep.

   Tip: Use the CTRL and SHIFT keys to select multiple lines or a range.
4. On the **File** menu, select **Save**, and then click the **Close** button.

   Note: If you did not modify the active policy, you must manually apply the policy to make it active.

Verifying that the SecurityFusion Module is Working

Introduction

To verify that the SecurityFusion Module is working, you can check the status, and then look for specific SecurityFusion event statuses in the Status column of the Analysis tab.

Note: You can find a list of statuses in the SiteProtector Help.

Prerequisites

If the Module does not appear to be working, make sure that you have met the following requirements:

- You must have specified hosts for the Module to correlate.
- You must have enabled impact analysis and attack pattern correlation in the SecurityFusion policy.

  Note: All Module functions are enabled by default at installation.
- SiteProtector must be collecting the vulnerability and IDS data for the specified hosts.

  Note: If you have not already set up SiteProtector to scan and monitor hosts, see "Vulnerability and IDS/IPS Data" in the SiteProtector Help.

Procedure

To verify that the Module is working:

1. In the left pane, select the group that contains the SecurityFusion Module.
2. In the View list, select Agent.
3. In the right pane, verify that the Status column for the module indicates *Active*.

   Note: The Status column can indicate an *Active*, *Stopped*, or *Offline* status for the Module.
4. In the View list, select Analysis.
5. Verify that statuses appear in the Status column:

   Note: The following status are determined by agents and may appear regardless of whether the SecurityFusion Module is working:

   - Failed attack (blocked by Proventia appliance)
   - Failure likely (rolled-back change)
   - Simulated block (Proventia appliance in simulation mode) statuses

Verifying operating status

Table 7 includes a list of statuses and descriptions that might appear in the Status column, which indicates that the SecurityFusion Module is working.

Status	Definition
Unknown impact (no correlation)	The impact of the event is unknown because no asset data (vulnerability or operating system) corresponds to this event. These events could be audit events, such as "login successful," status events from agents, or in some cases, events that the SecurityFusion Module does not correlate.
Success likely (target vulnerable)	A vulnerability assessment scan indicates that the asset was vulnerable to this attack, so the attack was probably successful.
Failure likely (no vulnerability)	A vulnerability assessment scan indicates that the asset was not vulnerable to this attack, so the attack probably failed.
Failure possible (scanned, vulnerability not confirmed)	Internet Scanner ran the correlating vulnerability check against the target, but the target did not confirm for certain whether the vulnerability exists.
Unknown impact (not scanned recently)	For one of the following reasons, no vulnerability or other asset data is available to determine the impact of the attack: The asset has never been scanned. The scan data for the asset has passed the user-defined expiration date.
Successful attack (confirmed by sensor)	The attack succeeded because the agent protecting the asset did not block the attack. If the attack was blocked (and failed), the agent confirms the attack by setting a flag inside the generated event.
Failed attack (confirmed by sensor)	The attack failed because the agent protecting the asset blocked the attack. The agent confirms the failure by setting a flag inside the generated event.
Failure likely (wrong OS)	The asset is running an operating system that is not susceptible to this attack.
Unknown impact (OS check indeterminate)	The impact of the attack is unknown because the vulnerability assessment scan could not determine the operating system of the target.
Unknown impact (SecurityFusion not enabled)	The SecurityFusion Module is not enabled for this Site or for this asset.
Unknown impact (SecurityFusion not configured for host)	The SecurityFusion Module is not configured for the host.

Table 7: *SecurityFusion Module statuses*

Note: If Unknown impact (SecurityFusion not enabled) appears in the Status column, then Event Collector is not configured correctly; or, in a multi-Event Collector environment, at least one Event Collector is not configured correctly.

SECTION D: Configuring Responses

Overview

Introduction

This section provides information about configuring response policies for the SecurityFusion Module.

Note: The Event Collector generates responses for the SecurityFusion Module.

Before you begin

Before you can configure email, SNMP, or user-specified responses for SecurityFusion Module, you must complete the following tasks:

- create a Event Collector response file
- apply the Event Collector response file to each Event Collector

Reference: For information about these tasks, see the *SiteProtector Help*.

In this section

This section contains the following topics:

Adjusting Severity Based on Event Impact

Introduction

You can configure the SecurityFusion Module to change the severity of correlated events as follows:

- to reduce false alarms, lower the severity
- to emphasize an attack, raise the severity

Default response

The default is to use the response set by the sensor policy.

Attacks that fail or failure is likely

Table 8 describes the severity adjustment options (in the **Adjust severity to** list) for events that fail or are likely to fail:

Option	Description
Low	Sets the severity of the event to Low.
Medium	Sets the severity of the event to Medium.
(One level lower)	Sets the severity of the event to one level lower than the original severity.
(Do not adjust)	Does not change the severity of the event. **Note:** This is the default response.

Table 8: *Severity options for events likely to fail*

Attacks that succeed or success is likely

Table 9 describes the severity adjustment options (in the **Adjust severity to** list) for events that succeed or are likely to succeed:

Option	Description
High	Sets the severity of the event to High.
Medium	Sets the severity of the event to Medium.
(One level lower)	Sets the severity of the event to one level lower than the original severity.
(Do not adjust)	Does not change the severity of the event. **Note:** This is the default response.

Table 9: *Severity options for events likely to succeed*

Displaying Events in the Console

Introduction

You can configure the SecurityFusion Module to display or not display correlated events in Console as follows:

- to reduce false alarms, do not display the event
- to emphasize an attack, display the event

Default response

The default is to use the response set by the sensor policy.

Display options

Table 10 describes the options (in the **Modify DISPLAY to list**) for displaying correlated events:

Option	Description
Off	Does not display the event in Site Protector.
On	Displays the event in Site Protector. **Important:** You must turn on DISPLAY and LOGDB before Site Protector can display events.
(Do not adjust)	Uses the response that is set for the sensor in the sensor policy.

Table 10: *Display Options for correlated events*

Logging Events to the SiteProtector Database

Introduction

You can configure whether or not to save correlated events in the SiteProtector Database (LOGDB). Use this response to ensure that you save only important events—regardless of the sensor response.

Default response

The default is to use the response set by the sensor policy.

Logging options

Table 11 describes the options (in the **Modify LOGDB to** list) for saving correlated events in the Site DB:

Option	Description
Off	Does not log the event to the Site DB.
On	Logs the event to the Site DB. **Important:** You must turn on both DISPLAY and LOGDB before SiteProtector can display events in the Site Manager.
(Do not adjust)	Uses the response that is set for the sensor in the sensor policy.

Table 11: *Logging options for correlated events*

Configuring Email and SNMP Responses

Introduction

You can configure the SecurityFusion Module to emphasize correlated events by sending email and SNMP responses.

Default response

Email and SNMP responses are not sent unless you configure them.

Prerequisites

To send email and SNMP responses, you must have already performed the following:

- created a custom policy file for the SecurityFusion Module
- created a custom response file for the Event Collector and sent to the Event Collector
- specified in the SecurityFusion custom policy the response from the Event Collector's response file
- applied the SecurityFusion custom policy to the SecurityFusion Module

Note: The name of the default SecurityFusion response file is `Event Collector Response.Policy`.

Procedure

To configure an email or an SNMP response:

1. Open your custom SecurityFusion policy for editing.
2. In the left pane, expand **Impact Analysis Component Settings**.
3. Do one of the following:
   - To change the response for failed attacks, select **Responses for Failed Attacks**.
   - To change the response for successful attacks, select **Responses for Successful Attacks**.
4. Select the check box next to the type or response you want to send:
   - EMAIL
   - SNMP
5. Does an arrow appear in the **Response Name** column?
   - If *yes*, go to Step 6.
   - If *no*, go to Step 7.
6. If you want to choose a different response, click the arrow, and then select another response.

   The name of the response you chose appears in the **Response Name** column.
7. If you want to make additional policy changes, refer to the following topics in the SiteProtector Help:
   - Overview: SecurityFusion Licensing
   - Overview: Managing Vulnerability Data
   - Overview: Responses Based on Event Impact

8. On the **File** menu, select **Save**, and then click the **Close** button.

   One of the following occurs:

   - If you modified the active policy, either a job automatically starts to apply the policy or a prompt appears for you to choose whether to apply the policy.
   - If you did not modify the active policy, you must apply the policy manually to make it active.

Configuring User-Specified Responses

Introduction	You can configure the SecurityFusion Module to run system commands or your own programs in response to correlated events.
Default response	User-specified responses are not taken unless you configure them.
Prerequisite	You must copy the custom program file to the sensors you want to run the program from.

Responding to Server Sensor Correlated Events

Introduction

For a small number of events, server sensor automatically correlates the event with host vulnerability data. By default, the SecurityFusion Module applies its responses to these events.

Background

In a small number of server sensor signatures (starting with version 6.5), the server sensor correlates events with host vulnerability data and determines a vulnerability status. In the server sensor policy, however, you cannot configure different responses based on host vulnerability. Consequently, the responses for these events may not be consistent with those applied by the SecurityFusion Module for events with the same vulnerability status.

Procedure

To apply SecurityFusion responses to server sensor correlated events:

1. Open your custom SecurityFusion policy for editing.
2. In the left pane, expand **Impact Analysis Component Settings.**
3. Select **Options.**
4. Select the **Apply SecurityFusion logic to server sensor alerts that correlate vulnerability information at the server** check box.
5. On the **File** menu, select **Save**, and then click the **Close** button.

   Note: If you did not modify the active policy, you must manually apply the policy to make it active.

SECTION E: Additional Configuration Tasks

Overview

Introduction

The SecurityFusion Module provides additional settings that you can configure based on your Site needs.

In this section

This section contains the following topics:

Configuring Vulnerability Data

Introduction

The SecurityFusion Module requires current host vulnerability assessment data to accurately estimate the impact of events. Depending on your requirements, you can configure how the Module uses vulnerability assessment data and how long the Module considers it as current.

Task overview

Table 12 describes the tasks for configuring vulnerability assessment data:

Task	Description
1	Limit how long the SecurityFusion Module considers scanned vulnerability assessment data as up-to-date and uses it to correlate events.
2	For Sites that use both network- and host-based scanners, choose whether to use the most recent scan data or the data from either the network- or host-based scanner when both are available.
3	Scan the hosts that you want to protect with SecurityFusion correlation.

Table 12: *Tasks for configuring vulnerability assessment data*

Ensuring current assessment data

To ensure that your vulnerability data is current, you can set up the Module to ignore data that is older than a certain agent in your Site. Then you should set up your scanning schedule to scan your hosts before vulnerability data expires. The default setting is 60 days.

How this option works—impact on event status

The Module checks the age of the vulnerability and operating system data for each event, and then does one of the following:

- If the data has not expired, the Module correlates the event.
- If the data has expired, the Module returns the status of Unknown impact (not scanned recently) and does not correlate the event.

Choosing a default vulnerability data source

By default, the SecurityFusion Module uses the most recent vulnerability data available (on a check-by-check basis), whether the data is from a network-based or host-based scanner. You can, however, configure the Module to use one source of data over the other if both are available and current.

Customizing Parameters for Attack Patterns

Introduction

This topic explains how to perform the following tasks:

- enable all or selected attack patterns in the SecurityFusion Module policy
- define configurable options for individual attack patterns

Types of attacks

The SecurityFusion Module searches for attack patterns and identifies attacks that involve more than one event. For supported attack patterns, the SecurityFusion Module eliminates the manual task of searching a long list of events to determine which ones are related.

The SecurityFusion Module correlates the following types of attack patterns:

- attacks that compromise hosts
- probing attacks that may include evasion or break-in activity
- break-in attacks against one or more hosts
- denial of Service attacks
- suspicious log-on activity

For a complete description of attack patterns, see the SecurityFusion policy.

Encrypting Communications with the Site Protector Database

Introduction

The SecurityFusion Module exchanges data with the SiteProtector database. By default, attack data is always encrypted; vulnerability correlation and other miscellaneous administrative data is not.

If required at your Site, you can set up encryption to include all types of data. You can use either Multiprotocol or SSL (Secure Sockets Layer) methods.

Important prerequisite

Before you encrypt communications for the SecurityFusion Module, read the relevant documentation:

- For Multiprotocol, see the *SiteProtector Installation Guide.*
- For SSL, see "How do I set up Site Protector to use encryption for database communication?" in the *Internet Security Systems Knowledgebase* (`http://iss.custhelp.com`

  To find the article:

  - Type `1824` in the Search Text box, and select Answer ID in the Search by list.

L

REDACTED

M

REDACTED